UNIT –III

ENGINEER'S RESPONSIBILITY FOR SAFETY

Syllabus: Safety and risk - assessment of safety and risk - risk benefit analysis and reducing risk - the three mile island and chernobyl case studies.

SAFETY AND RISK

Risk is a key element in any engineering design.

Concept of Safety:

A thing is safe if its risks are judged to be acceptable. Safety are tactily value judgments about what is acceptable risk to a given person or group.

Types of Risks:

Voluntary and Involuntary Risks

Short term and Long Term Consequences

Expected Portability

Reversible Effects

Threshold levels for Risk

Delayed and Immediate Risk

Risk is one of the most elaborate and extensive studies. The site is visited and exhaustive discussions with site personnel are undertaken. The study usually covers risk identification, risk analysis, risk assessment, risk rating, suggestions on risk control and risk mitigation.

Interestingly, risk analysis can be expanded to full fledge risk management study. The risk management study also includes residual risk transfer, risk financing etc. ***Stepwise, Risk Analysis will include:***

- Hazards identification
- Failure modes and frequencies evaluation from established sources and best practices.
- Selection of credible scenarios and risks.
- Fault and event trees for various scenarios.
- Consequences - effect calculations with work out from models.
- Individual and societal risks.
- ISO risk contours superimposed on layouts for various scenarios.
- Probability and frequency analysis.
- Established risk criteria of countries, bodies, standards.
- Comparison of risk against defined risk criteria.
- Identification of risk beyond the location boundary, if any.
- Risk mitigation measures.

The steps followed are need based and all or some of these may be required from the above depending upon the nature of site/plant.

Risk Analysis is undertaken after detailed site study and will reflect Chilworth exposure to various situations. It may also include study on frequency analysis, consequences analysis, risk acceptability analysis etc., if required. Probability and frequency analysis covers failure modes and frequencies from established sources and best practices for various scenarios and probability estimation.

Consequences analysis deals with selection of credible scenarios and consequences effect calculation including worked out scenarios and using software package.

RISK BENEFIT ANALYSIS AND REDUCING RISK

Risk-benefit analysis is the comparison of the risk of a situation to its related benefits.

For research that involves more than minimal risk of harm to the subjects, the investigator must assure that the amount of benefit clearly outweighs the amount of risk. Only if there is favorable risk benefit ratio, a study may be considered ethical.

Risk Benefit Analysis Example

Exposure to personal risk is recognized as a normal aspect of everyday life. We accept a certain level of risk in our lives as necessary to achieve certain benefits. In most of these risks we feel as though we have some sort of control over the situation. For example, driving an automobile is a risk most people take daily. "The controlling factor appears to be their perception of their individual ability to manage the risk-creating situation." Analyzing the risk of a situation is, however, very dependent on the individual doing the analysis. When individuals are exposed to involuntary risk, risk which they have no control, they make risk aversion their primary goal. Under these circumstances individuals require the probabilty of risk to be as much as one thousand times smaller then for the same situation under their perceived control.

Evaluations of future risk:

- Real future risk as disclosed by the fully matured future circumstances when they develop.
- Statistical risk, as determined by currently available data, as measured actuarially for insurance premiums.
- Projected risk, as analytically based on system models structured from historical studies.
- Perceived risk, as intuitively seen by individuals.

Air transportation as an example:

- Flight insurance company - statistical risk.
- Passenger - percieved risk.
- Federal Aviation Administration(FAA) - projected risks.

How to Reduce Risk?

1.Define the Problem

2.Generate Several Solutions

3. Analyse each solution to determine the pros and cons of each

4. Test the solutions

5.Select the best solution

6. Implement the chosen solution

7. Analyse the risk in the chosen solution

8. Try to solve it. Or move to next solution.

Risk-Benefit Analysis and Risk Management

Informative risk-benefit analysis and effective risk management are essential to the ultimate commercial success of your product. We are a leader in developing statistically rigorous, scientifically valid risk-benefit assessment studies that can be used to demonstrate the level of risk patients and other decision makers are willing to accept to achieve the benefits provided by your product.

Risk-Benefit Modeling	Systematically quantify the relative importance of risks and benefits to demonstrate the net benefits of treatment
Risk-Benefit Tradeoffs	Quantify patients' maximum acceptable risk for specific therapeutic benefits

CHERNOBYL CASE STUDIES

What Happened?

At 1:24 AM on April 26, 1986, there was an explosion at the Soviet nuclear power plant at Chernobyl. One of the reactors overheated, igniting a pocket of hydrogen gas. The explosion blew the top off the containment building, and exposed the molten reactor to the air. Thirty-one power plant workers were killed in the initial explosion, and radioactive dust and debris spewed into the air.

It took several days to put out the fire. Helicopters dropped sand and chemicals on the reactor rubble, finally extinguishing the blaze. Then the Soviets hastily buried the reactor in a sarcophagus of concrete. Estimates of deaths among the clean-up workers vary widely. Four thousand clean-up workers may have died in the following weeks from the radiation.

The countries now known as Belarus and Ukraine were hit the hardest by the radioactive fallout. Winds quickly blew the toxic cloud from Eastern Europe into Sweden and Norway. Within a week, radioactive levels had jumped over all of Europe, Asia, and Canada. It is estimated that seventy-thousand Ukrainians have been disabled, and five million people were exposed to radiation. Estimates of total deaths due to radioactive contamination range from 15,000 to 45,000 or more.

To give you an idea of the amount of radioactive material that escaped, the atomic bomb dropped on Hiroshima had a radioactive mass of four and a half tons. The exposed radioactive mass at Chernobyl was fifty tons.

In the months and years following, birth defects were common for animals and humans. Even the leaves on the trees became deformed.

Today, in Belarus and Ukraine, thyroid cancer and leukemia are still higher than normal. The towns of Pripyat and Chernobyl in the Ukraine are ghost towns. They will be uninhabitable due to radioactive contamination for several hundred years. The worst of the contaminated area is called "The Zone," and it is fenced off. Plants, meat, milk, and water in the area are still unsafe. Despite the contamination, millions of people live in and near The Zone, too poor to move to safer surroundings.

Further, human genetic mutations created by the radiation exposure have been found in children who have only recently been born. This suggests that there may be another whole generation of Chernobyl victims.

Recent reports say that there are some indications that the concrete sarcophagus at Chernobyl is breaking down.

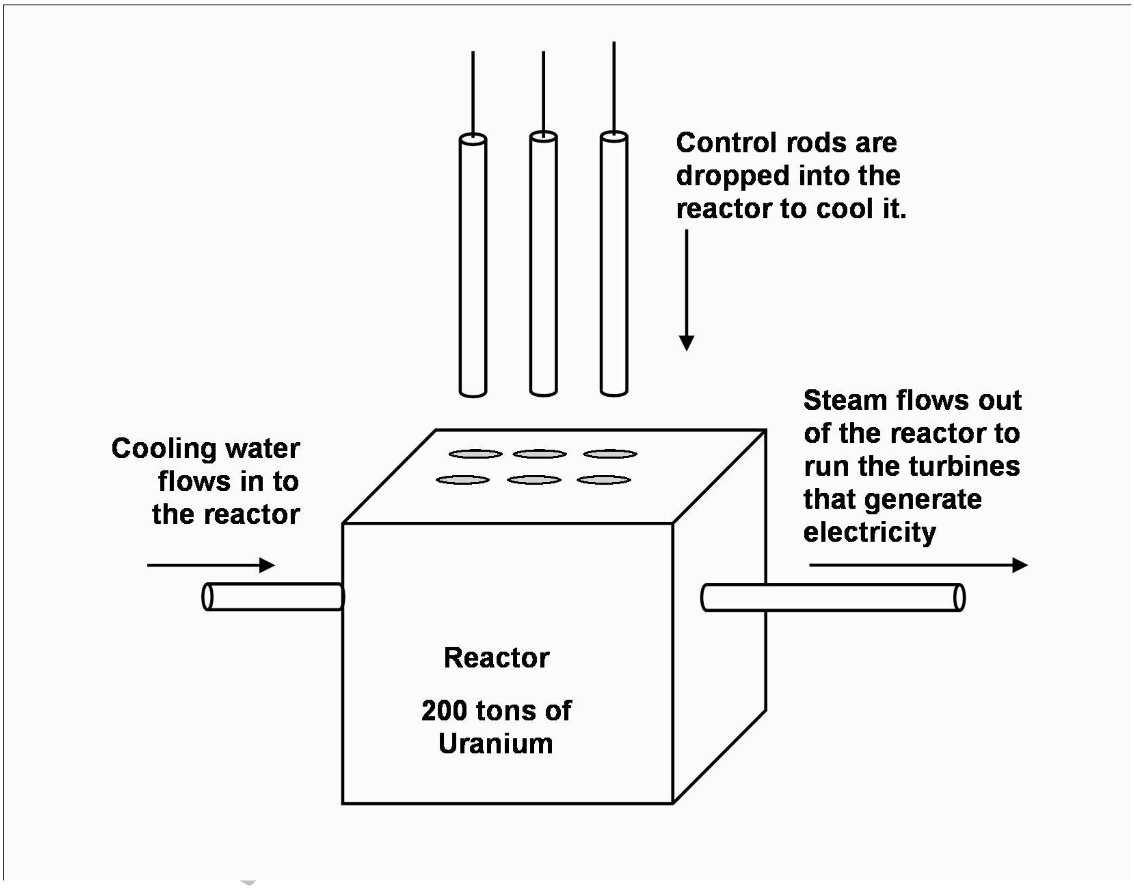
How a Nuclear Power Plant Works

The reactor at Chernobyl was composed of almost 200 tons of uranium. This giant block of uranium generated heat and radiation. Water ran through the hot reactor, turning to steam. The steam ran the turbines, thereby generating electricity. The hotter the reactor, the more electricity would be generated.

Left to itself, the reactor would become too *reactive*—it would become hotter and hotter and more and more radioactive. If the reactor had nothing to cool it down, it would quickly *meltdown*—a process where the reactor gets so hot that it melts—melting through the floor. So, engineers needed a way to control the temperature of the reactor, to keep it from the catastrophic meltdown. Further, the engineers needed to be able to regulate the temperature of the reactor—so that it ran hotter when more electricity was needed, and could run colder when less electricity was desired.

The method they used to regulate the temperature of the reactor was to insert heat-absorbing rods, called *control rods*. These control rods absorb heat and radiation. The rods hang above the reactor, and can be lowered into the reactor, which will cool the reactor. When more electricity is needed, the rods can be removed from the reactor, which will allow the reactor to heat up. The reactor has hollow tubes, and the control rods are lowered into these reactor tubes, or raised up out of the reactor tubes. At the Chernobyl-type reactors, there are 211 control rods. The more control rods that are inserted, the colder the reactor runs. The more control rods that are removed, the hotter the reactor becomes.

How a Nuclear Power Plant Works



Soviet safety procedures demanded that at least 28 rods were inserted into the Chernobyl reactor at all times. This was a way to make sure that the reactor wouldn't overheat.

Water was another method to moderate the temperature of the reactor. When more water ran through the reactor, the reactor cooled faster. When less water ran through the reactor, the reactor stayed hot.

Chernobyl Background

The list of senior engineers at Chernobyl was as follows: Viktor Bryukhanov, the plant director, was a pure physicist, with no nuclear experience.

Anatoly Dyatlov, the deputy chief engineer, served as the day-to-day supervisor. He had worked with reactor cores but had never before worked in a nuclear power plant. When he accepted the job as deputy chief engineer, he exclaimed, “you don’t have to be a genius to figure out a nuclear reactor.”

The engineers were Aleksandr Akimov, serving his first position in this role; Nikolai Fomin, an electrical engineer with little nuclear experience; Gennady Metlenko, an electrical engineer; and Leonid Toptunov, a 26 year-old reactor control engineer. The engineers were heavy in their experience of electric technology, but had less experience with the uniqueness of neutron physics.

The confidence of these engineers was exaggerated. They believed they had decades of problem-free nuclear work, so they believed that nuclear power was very safe. The engineers believed that they could figure out any problem. In reality, there had been many problems in the Soviet nuclear power industry. The Soviet state tried to keep problems a secret because problems are bad PR.

The Soviets had a number of nuclear accidents (this is a partial list of Soviet accidents before Chernobyl). In 1957 in Chelyabinsk, there was a substantial release of radioactivity caused by a spontaneous reaction in spent fuel; in 1966 in Melekess the nuclear power plant experienced a spontaneous surge in power, releasing radiation; In 1974, there was an explosion at the nuclear power plant in Leningrad; Later in 1974, at the same nuclear power plant, three people were killed and radiation was released into the environment; in 1977, there was a partial meltdown of nuclear fuel at Byeloyarsk; in 1978 at Byeloyarsk, the reactor went out of control after a roof panel fell onto it; In 1982 at Chernobyl, radioactivity was released into the environment; In 1982, there was there was a fire at Armyanskaya; In 1985, fourteen people were killed when a relief valve burst in Balakovo.

Had the engineers at Chernobyl had the information of the previous nuclear accidents, perhaps they would have known to be more careful. It is often from mistakes that we learn, and the engineers at Chernobyl had no opportunity to learn.

As a footnote, don’t think that the problems were just those mistake-laden Soviets. Here is a partial list of American accidents before Chernobyl: In 1951, the Detroit reactor overheated, and air was contaminated with radioactive gasses; In 1959, there was a partial meltdown in Santa Susanna, California; In 1961, three people were killed in an explosion at the nuclear power plant at Idaho Falls, Idaho; In 1966, there was a partial meltdown at a reactor near Detroit; In 1971, 53,000 gallons of radioactive water were released into the Mississippi River from the Monticello plant in Minnesota; In 1979, there was population evacuation and a discharge of radioactive gas and water in a partial meltdown at Three Mile Island; in 1979 there was a discharge of radiation in Irving Tennessee; In 1982, there was a release of radioactive gas into the environment in Rochester, New York; In 1982, there was a leak of radioactive gasses into the atmosphere at Ontario, New York; In 1985, there was a leak of radioactive water near New York City; In 1986, one person was killed in an explosion of a tank of radioactive gas in Webbers Falls, Oklahoma.

The engineers at Chernobyl didn't know about these nuclear accidents. These were secrets that the Soviets kept from the nuclear engineers. Consequently, no one was able to learn from the mistakes of the past. The nuclear plant staff believed that their experience with nuclear power was pretty much error-free, so they developed an overconfidence about their working style.

So, according to Gregori Medvedev (the Soviet investigator of Chernobyl), their practice became lazy and their safety practices slipshod. Further, the heavy bureaucracy and hierarchy of the Soviet system created an atmosphere where every decision had to be approved at a variety of higher levels. Consequently, the hierarchical system had quelled the operators' creativity and motivation for problem-solving.

April 25th, 1:00 PM

The engineers at Chernobyl had volunteered to do a safety test proposed by the Soviet government. In the event of a reactor shutdown, a back-up system of diesel generators would crank up, taking over the electricity generation. However, the diesel engines took a few minutes to start producing electricity. The reactor had a turbine that was meant to generate electricity for a minute or two until the diesel generators would start operating. The experiment at Chernobyl was meant to see exactly how long that turbine would generate the electricity.

The experiment required that the reactor be operating at 50% of capacity. On April 25th, 1986, at 1:00 PM, the engineers began to reduce the operating power of the reactor, by inserting the control rods into the reactor. This had the effect, you may recall, of cooling off the reactor—making it less reactive.

They also shut down the emergency cooling system. They were afraid that the cooling system might kick in during the test, thereby interfering with the experiment. They had no authorization to deactivate the cooling system, but they went ahead and deactivated it.

The experiment called for running the reactor at 50% capacity, thereby generating only half the electricity. At 2:00 PM, a dispatcher at Kiev called and asked them to delay the test because of the higher-than-expected energy usage. They delayed the test, but did not reactivate the emergency cooling system.

April 25th, 11:00 PM

At 11:00 PM, they began the test again. Toptunov, the senior reactor control engineer, began to manually lower the reactor to 50% of its capacity so that they could begin the turbine safety experiment.

Lowering the power generation of a nuclear reactor is a tricky thing. It is not like lowering the thermostat in a house. When you lower the thermostat in the house from 72 to 68 degrees, the temperature in the house will drop to 68 degrees and stay there. But in a nuclear reactor,

the dropping of the temperature is not only the *result* of lowering the reactivity, but it is also a *cause* of lowering the reactivity. In other words, the coldness of the reactor will make the reactor colder. This is called the *self-damping effect*. Conversely, when the reactor heats up, the heat of the reactor will make itself hotter (the self-amplifying effect).

So, when the control rods are dropped into the reactor, the reactivity goes down. And the water running through the reactor also lessens reactivity. But the lower reactivity also makes the reactor itself less reactive. So, the Chernobyl reactor damped itself, even as the water and the control rods damped its reactivity.

It is typically hard for people to think in terms of exponential reduction or exponential increase. We naturally think of a linear (straight-line) reduction or a linear increase. We have trouble with self-damping and self-amplifying effects, because they are nonlinear by definition.

So, the engineers oversteered the process, and hit the 50% mark, but they were unable to keep it there. By 12:30 AM, the power generation had dropped to 1% of capacity.

Chernobyl-type reactors are not meant to drop that low in their capacity. There are two problems with the nuclear reactor running at 1% of capacity. When reactivity drops that low, the reactor runs unevenly and unstably, like a bad diesel engine. Small pockets of reactivity can begin that can spread hot reactivity through the reactor. Secondly, the low running of the reactor creates unwanted gasses and byproducts (xenon and iodine) that poison the reactor. Because of this, they were strictly forbidden to run the reactor below 20% of capacity.

In the Chernobyl control room, Dyatlov (the chief engineer in charge of the experiment), upon hearing the reactor was at 1%, flew into a rage. With the reactor capacity was so low, he would not be able to conduct his safety experiment. With the reactor at 1% capacity, Dyatlov had two options:

1. One option was to let the reactor go cold, which would have ended the experiment, and then they would have to wait for two days for the poisonous byproducts to dissipate before starting the reactor again. With this option, Dyatlov would no doubt have been reprimanded, and possibly lost his job.
2. The other option was to immediately increase the power. Safety rules prohibited increasing the power if the reactor had fallen from 80% capacity. In this case, the power had fallen from 50% capacity—so they were not technically governed by the safety protocols.

Dyatlov ordered the engineers to raise power.

Today, we know the horrible outcome of this Chernobyl chronology. It is easy for us to sit back in our armchairs, with the added benefit of hindsight, and say Dyatlov made the wrong choice. Of course, he could have followed the spirit of the protocols and shut the reactor down. However, Dyatlov did not have the benefit of hindsight. He was faced with the choice of the *surety* of reprimand and the harming of his career vs. the *possibility* of safety problems. And, we know from engineers and technical operators everywhere, safety protocols are *routinely* breached when faced with this kind of choice. Experts tend to believe that they are experts, and that the safety rules are for amateurs.

Further, safety rules are not designed so that people are killed instantly when the safety standard is broken. On a 55-mile per hour limit on a highway, cars do not suddenly burst into flames at 56 miles per hour. In fact, there is an advantage to going 56 miles an hour as opposed to 55 (you get to your destination faster). In the same way, engineers frequently view safety rules as troublesome, and there is an advantage to have the freedom to disregard them.

In fact, we experience this psychologic every day, usually without thinking about it. When you come toward an intersection, and the light turns yellow, you reach a point where you either have to go through on a yellow light, or come to a stop. Many people go through on the yellow, even though there is a greater risk. So, in a split second, we decide between the surety of sitting at a red light or the possibility, albeit slight, of a safety problem to go through the yellow light. There is a clear advantage to take the risk (as long as you aren't in an accident). While the stakes were higher at Chernobyl, the same psychologic applies.

At this point in the Chernobyl process, there were 28 control rods in the reactor—the minimum required. Increasing power would mean that even more control rods would have to be removed from the reactor. This would be a breach of protocol--the minimum number of rods was 28. Dyatlov gave the order to remove more control rods.

Toptunov, the reactor control engineer, refused to remove any more rods. He believed it would be unsafe to increase the power. With the reactor operating at 1%, and the minimum number of control rods in the reactor, he believed it would be unsafe to remove more rods. He was abiding by a strict interpretation of the safety protocols of 28 rods.

But Dyatlov continued to rage, swearing at the engineers and demanding they increase power. Dyatlov threatened to fire Toptunov immediately if he didn't increase the power.

The 26-year-old Toptunov was faced with a choice. He believed he had two options:

1. He could refuse to increase power—but then Dyatlov would fire him immediately, and his career would be over.
2. His other choice was to increase power, recognizing that something bad *might* happen.

Toptunov looked around. All the other engineers—including his supervisors—were willing to increase power. Toptunov knew he was young and didn't have much experience with reactors. Perhaps this kind of protocol breach was normal. Toptunov was faced with that choice of the *surety* of his career ending, vs the *possibility* of safety problems. Toptunov decided to agree and increase the power.

Tragically, it would be the last decision Toptunov would ever make.

April 26th, 1:00 AM

By 1:00 AM, the power of the reactor was stable at 7% of capacity. Only 18 control rods were in the reactor (safety protocols demanded that no less than 28 control rods should always be in the reactor).

At 1:07 AM, the engineers wanted to make sure the reactor wouldn't overheat, so they turned on more water to ensure proper cooling (they were now pumping five times the normal rate of water through the reactor). The extra water cooled the reactor, and the power dropped again. The engineers responded by withdrawing even more control rods. Now, only 3 control rods were inserted in the reactor.

The reactor stabilized again. The engineers, satisfied with the amount of steam they were getting (they needed steam for their experiment) shut off the pumps for the extra water. They shut off the water, apparently only considering the effect that the water would have on the experiment—and did not consider the effect that the water was having on the reactor. At this point, with only 3 control rods in the reactor, the water was only thing keeping the reactor cool. Without the extra cool water, the reactor began to get hot. Power increased slowly at first. As the reactor got hotter, the reactor itself made the reactor hotter—the self-amplifying effect. The heat and reactivity of the reactor increased exponentially.

The engineers were trying to watch multiple variables simultaneously. The water, the steam, the control rods, and the current temperature of the reactor all were intertwined to affect the reactivity of the reactor. People can easily think in cause and effect terms. Had their only been one variable that controlled the reactivity, the results would probably have been different. However, people have difficulty thinking through the process when there are a multitude of variables, all interacting in different ways.

People are not processors of unlimited information. There is a limited amount of information with which a person can work. With the safety of hindsight, we can sit back and make a judgment saying, "they didn't think through all their information." However, this kind of linear judgment does not tell us *why* they didn't see what is obvious to our hindsight.

At 1:22 AM (90 seconds before the explosion), the engineers were still relaxed and confident. Dyatlov, in fact, was seeing his turbine safety experiment coming to a successful conclusion. In what turned out to be a tragic irony, he encouraged his engineers by suggesting, “in two or three minutes it will all be over.”

Thirty seconds before the explosion, the engineers realized the reactor was heating up too fast. With only 3 control rods in the reactor, and then shutting off the water, the reactor was superheating. In a panic, they desperately tried to drop control rods into the reactor, but the heat of the reactor had already melted the tubes into which the control rods slid.

The floor of the building began to shake, and loud banging started to echo through the control room. The coolant water began to boil violently, causing the pipes to burst. The super-heating reactor was creating hydrogen and oxygen gasses. This explosive mixture of gasses accumulated above the reactor. The heat of the reactor was building fast, and the temperature of the flammable gasses was rising.

April 26th, 1:24 AM

Finally, the gasses detonated, destroying the reactor and the protective containment building. The control room was far enough away from the containment building to escape destruction, but the explosion shook the entire plant. Debris caved in around the control room members, and Dyatlov, Akimov, Toptunov, and the others were knocked to the floor. Dust and chalk filled the air. While they knew there had been an explosion, they hoped and prayed the explosion had not come from the reactor. Toptunov and Akimov ran over the broken glass and ceiling debris to the open door, and ran across the compound toward the containment building. There, they saw the horrifying, unspeakable sight. There was rubble where the reactor had been. They saw flames shooting up 40 feet high, burning oil squirting from pipes onto the ground, black ash falling to the ground, and a bright purple light emanating from the rubble.

Within a few minutes, fire fighters had arrived. The fire fighters, most with no protective equipment, heroically worked to extinguish the fire, hoping to prevent further damage to the three other reactors at the plant. Most of the fire fighters died from the radiation exposure.

Bryukhanov (the plant director), who was not at the plant at the time, had been contacted and told about an explosion. In the chaos, those informing Bryukhanov of the explosion still did not know the total amount of devastation. Bryukhavov, still desperately hoping that the reactor was intact, called Moscow to inform them that while there had been an explosion, the reactor had not sustained any damage.

Again, with the benefit of hindsight, we can say that Bryukhanov should have acted quicker. It's true that many lives could have been saved if he had acted differently. However, his actions are not uncommon in these kinds of situations. A common reaction is called "horizontal flight," where people retreat from the worst-case scenario, convincing themselves to believe the best-case scenario. Bryukhanov had convinced himself that the reactor was not in danger. And after all, someone from the plant had called and given an ambiguous message. Surely they would have known if the reactor had been destroyed.

April 26th, 4:00 AM

At 4:00 AM, the command from Moscow came back: *Keep the reactor cool*. The authorities in Moscow had no idea that the damage was so catastrophic.

Akimov, Dyatlov, and Toptunov, their skin brown from the radiation, and their bodies wrenched from internal damage, had already been taken away to the medical center.

At 10:00 AM, Bryukhanov, the plant director, was informed that the reactor had been destroyed. Bryukhanov rejected the information, preferring to believe that the reactor was still intact. He informed Moscow that the reactor was intact and radiation was within normal limits.

Later that day, experts from around the Soviet Union came to Chernobyl, and found the horrifying truth. The reactor had indeed been destroyed, and fifty tons of radioactive fuel had instantly evaporated. The wind blew the radioactive plume in a northwesterly direction. Belarus and Finland were going to be in the path of the radioactive cloud.

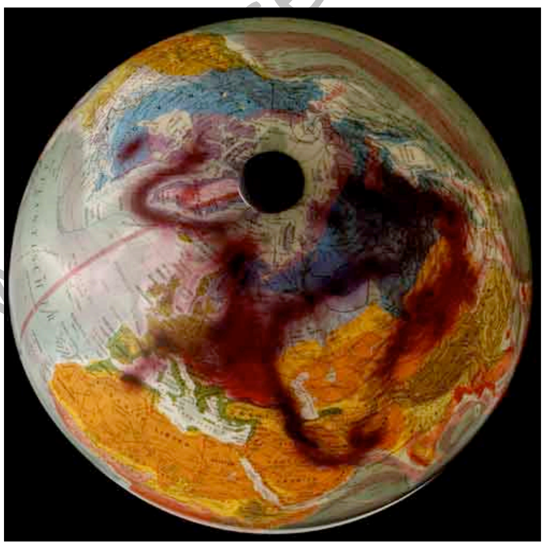
The Days Afterward

The secretive Soviet state was slow to act. Soviet bureaucracy debated whether to evacuate nearby cities, and how much land should be evacuated. They were slow in their response, slow to evacuate, and slow to inform the world of the disaster. It took over 36 hours before authorities began to evacuate nearby residents. Two days later, the nightly news (the fourth story) reported that one of the reactors was "damaged."

Within a few days, radiation detectors were going off all over the world. The Soviets continued to try to hide the issue from the world and their own residents.

Several months later, Bryukhanov was arrested, still believing that he did everything right. Dyatlov survived the radiation sickness, and was arrested in December of that year. He believed he was a scapegoat for the accident. Akimov died a few weeks after the disaster, but till the very end continued to say, "I did everything right. I don't know how it happened."

The radiation cloud on April 27th, 1986

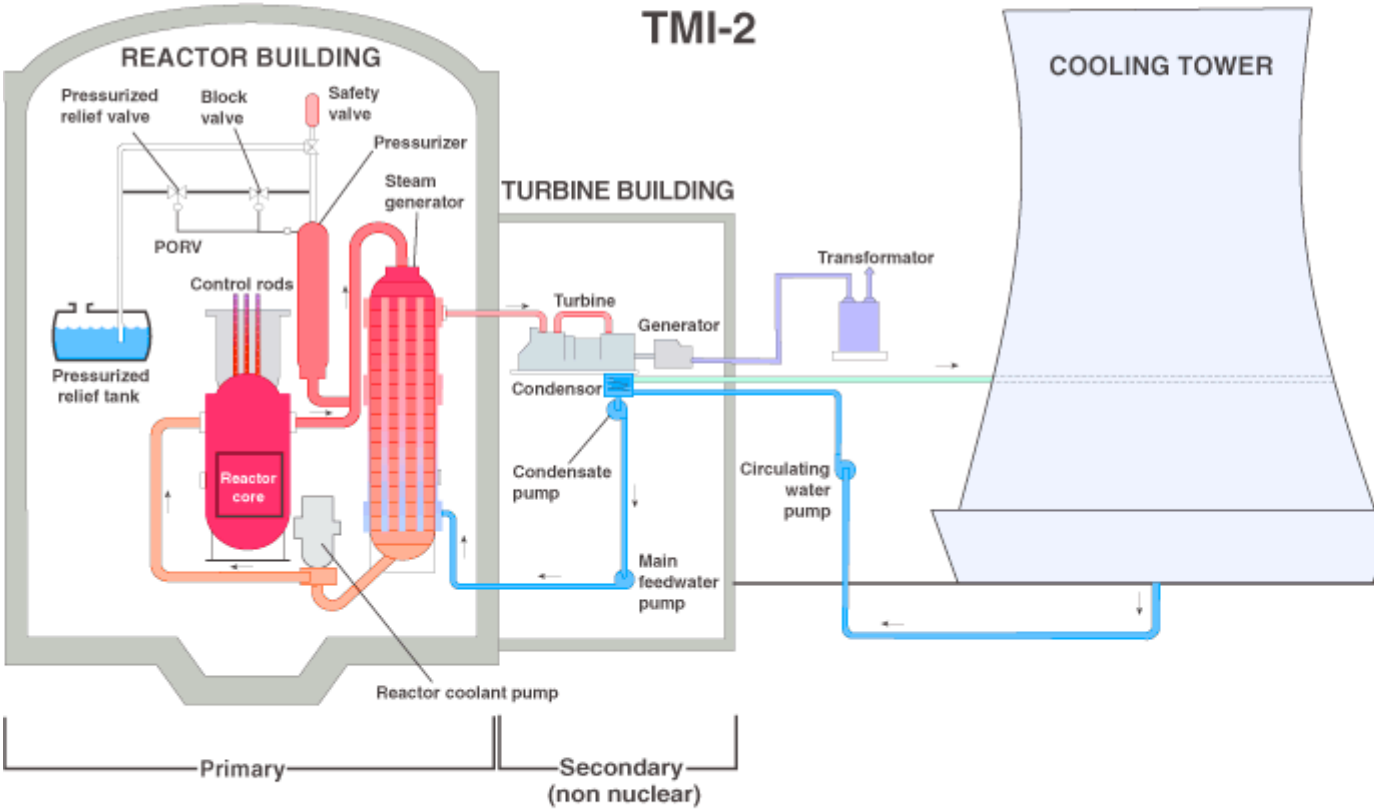


THREE MILE ISLAND ACCIDENT

(*March 2001*, *minor update Jan 2010*)

- **In 1979 at Three Mile Island nuclear power plant in USA a cooling malfunction caused part of the core to melt in the # 2 reactor. The TMI-2 reactor was destroyed.**
- **Some radioactive gas was released a couple of days after the accident, but not enough to cause any dose above background levels to local residents.**
- **There were no injuries or adverse health effects from the Three Mile Island accident.**

The Three Mile Island power station is near Harrisburg, Pennsylvania in USA. It had two pressurized water reactors. One PWR was of 800 MWe (775 MWe net) and entered service in 1974. It remains one of the best-performing units in USA. Unit 2 was of 906 MWe (880 MWe net) and almost brand new.



The accident to unit 2 happened at 4 am on 28 March 1979 when the reactor was operating at 97% power. It involved a relatively minor malfunction in the secondary cooling circuit which caused the temperature in the primary coolant to rise. This in turn caused the reactor to shut down automatically. Shut down took about one second. At this point a relief valve failed to close, but instrumentation did not reveal the fact, and so much of the primary coolant drained away that the residual decay heat in the reactor core was not removed. The core suffered severe damage as a result.

The operators were unable to diagnose or respond properly to the unplanned automatic shutdown of the reactor. Deficient control room instrumentation and inadequate emergency response training proved to be root causes of the accident

The chain of events during the Three Mile Island Accident

Within seconds of the shutdown, the pilot-operated relief valve (PORV) on the reactor cooling system opened, as it was supposed to. About 10 seconds later it should have closed. But it remained open, leaking vital reactor coolant water to the reactor coolant drain tank. The operators believed the relief valve had shut because instruments showed them that a "close" signal was sent to the valve. However, they did not have an instrument indicating the valve's actual position.

Responding to the loss of cooling water, high-pressure injection pumps automatically pushed replacement water into the reactor system. As water and steam escaped through the relief valve, cooling water surged into the pressuriser, raising the water level in it. (The pressuriser is a tank which is part of the primary reactor cooling system, maintaining proper pressure in the system. The relief valve is located on the pressuriser. In a PWR like TMI-2, water in the primary cooling system around the core is kept under very high pressure to keep it from boiling.)

Operators responded by reducing the flow of replacement water. Their training told them that the pressuriser water level was the only dependable indication of the amount of cooling water in the system. Because the pressuriser level was increasing, they thought the reactor system was too full of water. Their training told them to do all they could to keep the pressuriser from filling with water. If it filled, they could not control pressure in the cooling system and it might rupture.

Steam then formed in the reactor primary cooling system. Pumping a mixture of steam and water caused the reactor cooling pumps to vibrate. Because the severe vibrations could have damaged the pumps and made them unusable, operators shut down the pumps. This ended forced cooling of the reactor core. (The operators still believed the system was nearly full of water because the pressuriser level remained high.) However, as reactor coolant water boiled away, the reactor?s fuel core was uncovered and became even hotter. The fuel rods were damaged and released radioactive material into the cooling water.

At 6:22 am operators closed a block valve between the relief valve and the pressuriser. This action stopped the loss of coolant water through the relief valve. However, superheated steam and gases blocked the flow of water through the core cooling system.

Throughout the morning, operators attempted to force more water into the reactor system to condense steam bubbles that they believed were blocking the flow of cooling water. During the afternoon, operators attempted to decrease the pressure in the reactor system to allow a low pressure cooling system to be used and emergency water supplies to be put into the system.

Cooling Restored

By late afternoon, operators began high-pressure injection of water into the reactor cooling system to increase pressure and to collapse steam bubbles. By 7:50 pm on 28 March, they restored forced cooling of the reactor core when they were able to restart one reactor coolant pump. They had condensed steam so that the pump could run without severe vibrations.

Radioactive gases from the reactor cooling system built up in the makeup tank in the auxiliary building. During March 29 and 30, operators used a system of pipes and compressors to move the gas to waste gas decay tanks. The compressors leaked, and some radioactive gas was released to the environment.

The Hydrogen Bubble

When the reactor's core was uncovered, on the morning of 28 March, a high-temperature chemical reaction between water and the zircaloy metal tubes holding the nuclear fuel pellets had created hydrogen gas. In the afternoon of 28 March, a sudden rise in reactor building pressure shown by the control room instruments indicated a hydrogen burn had occurred. Hydrogen gas also gathered at the top of the reactor vessel.

From 30 March through 1 April operators removed this hydrogen gas "bubble" by periodically opening the vent valve on the reactor cooling system pressuriser. For a time, regulatory (NRC) officials believed the hydrogen bubble could explode, though such an explosion was never possible since there was not enough oxygen in the system.

Cold Shutdown

After an anxious month, on 27 April operators established natural convection circulation of coolant. The reactor core was being cooled by the natural movement of water rather than by mechanical pumping. The plant was in "cold shutdown".

Public concern and confusion

When the TMI-2 accident is recalled, it is often in the context of what happened on Friday and Saturday, March 30-31. The drama of the TMI-2 accident-induced fear, stress and confusion on those two days. The atmosphere then, and the reasons for it, are described well in the book "*Crisis Contained, The Department of Energy at Three Mile Island*," by Philip L Cantelon and Robert C. Williams, 1982. This is an official history of the Department of Energy's role during the accident.

"Friday appears to have become a turning point in the history of the accident because of two events: the sudden rise in reactor pressure shown by control room instruments on Wednesday afternoon (the "hydrogen burn") which suggested a hydrogen explosion? became known to the Nuclear Regulatory Commission [that day]; and the deliberate venting of radioactive gases from the plant Friday morning which produced a reading of 1,200 millirems (12 mSv) directly above the stack of the auxiliary building.

"What made these significant was a series of misunderstandings caused, in part, by problems of communication within various state and federal agencies. Because of confused telephone conversations between people uninformed about the plant's status, officials concluded that the 1,200 millirems (12 mSv) reading was an off-site reading. They also believed that another hydrogen explosion was possible, that the Nuclear Regulatory Commission had ordered evacuation and that a meltdown was conceivable.

"Garbled communications reported by the media generated a debate over evacuation. Whether or not there were evacuation plans soon became academic. What happened on

Friday was not a planned evacuation but a weekend exodus based not on what was actually happening at Three Mile Island but on what government officials and the media imagined might happen. On Friday confused communications created the politics of fear." (Page 50)

Throughout the book, Cantelon and Williams note that hundreds of environmental samples were taken around TMI during the accident period by the Department of Energy (which had the lead sampling role) or the then-Pennsylvania Department of Environmental Resources. But there were no unusually high readings, except for noble gases, and virtually no iodine. Readings were far below health limits. Yet a political storm was raging based on confusion and misinformation.

No Radiological Health Effects

The Three Mile Island accident caused concerns about the possibility of radiation-induced health effects, principally cancer, in the area surrounding the plant. Because of those concerns, the Pennsylvania Department of Health for 18 years maintained a registry of more than 30,000 people who lived within five miles of Three Mile Island at the time of the accident. The state's registry was discontinued in mid 1997, without any evidence of unusual health trends in the area.

Indeed, more than a dozen major, independent health studies of the accident showed no evidence of any abnormal number of cancers around TMI years after the accident. The only detectable effect was psychological stress during and shortly after the accident.

The studies found that the radiation releases during the accident were minimal, well below any levels that have been associated with health effects from radiation exposure. The average radiation dose to people living within 10 miles of the plant was 0.08 millisieverts, with no more than 1 millisievert to any single individual. The level of 0.08 mSv is about equal to a chest X-ray, and 1 mSv is about a third of the average background level of radiation received by U.S. residents in a year.

In June 1996, 17 years after the TMI-2 accident, Harrisburg U.S. District Court Judge Sylvia Rambo dismissed a class action lawsuit alleging that the accident caused health effects. The plaintiffs have appealed Judge Rambo's ruling. The appeal is before the U.S. Third Circuit Court of Appeals. However, in making her decision, Judge Rambo cited:

· Findings that exposure patterns projected by computer models of the releases compared so well with data from the TMI dosimeters (TLDs) available during the accident that the dosimeters probably were adequate to measure the releases.

· That the maximum offsite dose was, possibly, 100 millirem (1 mSv), and that projected fatal cancers were less than one.

· The plaintiffs' failure to prove their assertion that one or more unreported hydrogen "blowouts" in the reactor system caused one or more unreported radiation "spikes", producing a narrow yet highly concentrated plume of radioactive gases.

Judge Rambo concluded: "The parties to the instant action have had nearly two decades to muster evidence in support of their respective cases.... The paucity of proof alleged in support

of Plaintiffs' case is manifest. The court has searched the record for any and all evidence which construed in a light most favourable to Plaintiffs creates a genuine issue of material fact warranting submission of their claims to a jury. This effort has been in vain."

More than a dozen major, independent studies have assessed the radiation releases and possible effects on the people and the environment around TMI since the 1979 accident at TMI-2. The most recent was a 13-year study on 32,000 people. None has found any adverse health effects such as cancers which might be linked to the accident.

The TMI-2 Cleanup

The cleanup of the damaged nuclear reactor system at TMI-2 took nearly 12 years and cost approximately US$973 million. The cleanup was uniquely challenging technically and radiologically. Plant surfaces had to be decontaminated. Water used and stored during the cleanup had to be processed. And about 100 tonnes of damaged uranium fuel had to be removed from the reactor vessel -- all without hazard to cleanup workers or the public.

A cleanup plan was developed and carried out safely and successfully by a team of more than 1000 skilled workers. It began in August 1979, with the first shipments of accident-generated low-level radiological waste to Richland, Washington. In the cleanup's closing phases, in 1991, final measurements were taken of the fuel remaining in inaccessible parts of the reactor vessel. Approximately one percent of the fuel and debris remains in the vessel. Also in 1991, the last remaining water was pumped from the TMI-2 reactor. The cleanup ended in December 1993, when Unit 2 received a license from the NRC to enter Post Defueling Monitored Storage (PDMS).

Early in the cleanup, Unit 2 was completely severed from any connection to TMI Unit 1. TMI-2 today is in long-term monitored storage. No further use of the nuclear part of the plant is anticipated. Ventilation and rainwater systems are monitored. Equipment necessary to keep the plant in safe long-term storage is maintained.

Defueling the TMI-2 reactor vessel was the heart of the cleanup. The damaged fuel remained underwater throughout the defueling. In October 1985, after nearly six years of preparations, workers standing on a platform atop the reactor and manipulating long-handled tools began lifting the fuel into canisters that hung beneath the platform. In all, 342 fuel canisters were shipped safely for long-term storage at the Idaho National Laboratory, a program that was completed in April 1990.

TMI-2 cleanup operations produced over 10.6 megalitres of accident-generated water that was processed, stored and ultimately evaporated safely.

In February 1991, the TMI-2 Cleanup Program was named by the National Society of Professional Engineers as one of the top engineering achievements in the U.S. completed during 1990.

In 2010 the generator was sold by FirstEnergy to Progress Energy to upgrade its Harris nuclear power plant in North Carolina. It is being shipped in two parts, the rotor, which weighs 170 tonnes, and the stator, which weighs about 500 tonnes.

The NRC web site has a factsheet on Three Mile Island.

TMI-1: Safe and World-Class

From its restart in 1985, Three Mile Island Unit 1 has operated at very high levels of safety and reliability. Application of the lessons of the TMI-2 accident has been a key factor in the plant's outstanding performance.

In 1997, TMI-1 completed the longest operating run of any light water reactor in the history of nuclear power worldwide - 616 days and 23 hours of uninterrupted operation. (That run was also the longest at any steam-driven plant in the U.S., including plants powered by fossil fuels.) And in October 1998, TMI employees completed three million hours of work without a lost-work day accident.

At the time of the TMI-2 accident, TMI-1 was shut down for refueling. It was kept shut down during lengthy proceedings by the Nuclear Regulatory Commission. During the shutdown, the plant was modified and training and operating procedures were revamped in light of the lessons of TMI-2.

When TMI-1 restarted in October 1985, General Public Utilities pledged that the plant would be operated safely and efficiently and would become a leader in the nuclear power industry. Those pledges have been kept.

- The plant's capability factor for 1987, including almost three months of a five-month refueling and maintenance outage, was 74.1 percent, compared to an industry average of 62 percent. (Capability factor refers to the amount of electricity generated compared to the plant's maximum capacity.)
- In 1988 a 1.3% (11 MWe) uprate was licensed.
- For 1989, TMI-1's capability factor was 100.03 percent and the best of 357 nuclear power plants worldwide, according to *Nucleonics Week*.
- In 1990-91, TMI-1 operated 479 consecutive days, the longest operating run at that point in the history of US commercial nuclear power. It was named by the NRC as one of the four safest plants in the country during this period.
- By the end of 1994, TMI-1 was one of the first two plants in the history of US commercial nuclear power to achieve a three-year average capability factor of over 90% (TMI-1 had 94.3%).
- In October 1998, TMI workers completed two full years without a lost workday injury.
- Since its restart, TMI-1 has earned consistently high ratings in the NRC's program, Systematic Assessment of Licensee Performance (SALP).
- In 2009, the TMI-1 operating licence was renewed, extending it life by 20 years to 2034.
- Immediately following this, both steam generators were replaced as TMI's "largest capital project to date"

In 1999, TMI-1 was purchased by AmerGen, a new joint venture between British Energy and PECO Energy. In 2003 the BE share was sold so that the plant became wholly-owned by Exelon, PECO's successor. It is now listed as producing 786 MWe net.

Training improvements

Training reforms are among the most significant outcomes of the TMI-2 accident. Training became centred on protecting a plant's cooling capacity, whatever the triggering problem might be. At TMI-2, the operators turned to a book of procedures to pick those that seemed to fit the event. Now operators are taken through a set of "yes-no" questions to ensure, *first*, that the reactor's fuel core remains covered. *Then* they determine the specific malfunction. This is known as a "symptom-based" approach for responding to plant events. Underlying it is a style of training that gives operators a foundation for understanding both theoretical and practical aspects of plant operations.

The TMI-2 accident also led to the establishment of the Atlanta-based Institute of Nuclear Power Operations (INPO) and its National Academy for Nuclear Training. These two industry organisations have been effective in promoting excellence in the operation of nuclear plants and accrediting their training programs.

INPO was formed in 1979. The National Academy for Nuclear Training was established under INPO's auspices in 1985. TMI's operator training program has passed three INPO accreditation reviews since then.

Training has gone well beyond button-pushing. Communications and teamwork, emphasizing effective interaction among crew members, are now part of TMI's training curriculum.

Close to half of the operators' training is in a full-scale electronic simulator of the TMI control room. The $18 million simulator permits operators to learn and be tested on all kinds of accident scenarios.

Increased safety & reliability

Disciplines in training, operations and event reporting that grew from the lessons of the TMI-2 accident have made the nuclear power industry demonstrably safer and more reliable. Those trends have been both promoted and tracked by the Institute for Nuclear Power Operations (INPO). To remain in good standing, a nuclear plant must meet the high standards set by INPO as well as the strict regulation of the US Nuclear Regulatory Commission.

A key indicator is the graph of significant plant events, based on data compiled by the Nuclear Regulatory Commission. The number of significant events decreased from 2.38 per reactor unit in 1985 to 0.10 at the end of 1997.

On the reliability front, the median capability factor for nuclear plants - the percentage of maximum energy that a plant is capable of generating - increased from 62.7 percent in 1980 to almost 90 percent in 2000. (The goal for the year 2000 was 87 percent.)

Other indicators for US plants tracked by INPO and its world counterpart, the World Association of Nuclear Operators (WANO) are the unplanned capability loss factor, unplanned automatic scrams, safety system performance, thermal performance, fuel reliability, chemistry performance, collective radiation exposure, volume of solid radioactive waste and industrial safety accident rate. All are reduced, that is, improved substantially, from 1980.

Summary

What Happened:

- The TMI-2 reactor's fuel core became uncovered and more than one third of the fuel melted.
- Inadequate instrumentation and training programs at the time hampered operators' ability to respond to the accident.
- The accident was accompanied by communications problems that led to conflicting information available to the public, contributing to the public's fears
- Radiation was released from the plant. The releases were not serious and were not health hazards. This was confirmed by thousands of environmental and other samples and measurements taken during the accident.
- The containment building worked as designed. Despite melting of about one-third of the fuel core, the reactor vessel itself maintained its integrity and contained the damaged fuel.

What did not Happen:

- There was no "China Syndrome".
- There were no injuries or detectable health impacts from the accident, beyond the initial stress.

Longer-Term Impacts:

- Applying the accident's lessons produced important, continuing improvement in the performance of all nuclear power plants.
- The accident fostered better understanding of fuel melting, including improbability of a "China Syndrome" meltdown breaching the reactor vessel or the containment building.
- Public confidence in nuclear energy, particularly in USA, declined sharply following the Three Mile Island accident. It was a major cause of the decline in nuclear construction through the 1980s and 1990s.